Special Topics in Mathematics
(MATH 4613)
Cryptography
Fall 2007

Professor: Paul Bailey

Office: WIL 228

Office Hours: MTWRF 11 am to 12 noon; MWF 1 pm to 2 pm

Web Site: `http://www.saumag.edu/pbailey`

Email: `plbailey@saumag.edu`

Text: *Introduction to Cryptography*, 2$^{\text{nd}}$ edition, by Trappe and Washington

Grade Components

Software:	40%
Problems:	10%
Quizzes:	10%
Midterm:	15%
Final:	25%

Software consists of programming projects which will be assigned periodically. The programs are to be written in C++, compilable under Microsoft Visual Studio .NET (although you may use another editor/compiler when designing the program, if you wish). The completed program source code is to be emailed to `plbailey@saumag.edu`.

Problems which are mathematical in nature will be assigned occasionally. Complete solutions should be written neatly in complete sentences and paragraphs.

Quizzes will be occasionally given in class on Friday. These consist of one or two problems, and should be completed in twenty minutes.

The *Midterm* examination will be given around the third week in October.

The *Final* examination is scheduled by the university.

Course Outline

Week	Beginning	Topic	Sections
Week 1	Aug 27	Shift and Affine Cyphers	2.1, 2.2
Week 2	Sep 3	Substitution Cyphers	2.4, 2.5
Week 3	Sep 10	Vignere Cyphers	2.1, 2.2, 2.3, 2.4
Week 4	Sep 17	Block Cyphers	2.7
Week 5	Sep 24	Feistel Cyphers	4.1, 4.2
Week 6	Oct 1	DES	4.4
Week 7	Oct 8	AES	5.1, 5.2, 5.3
Week 8	Oct 15	RSA	6.1
Week 9	Oct 22	Primality Testing	6.3
Week 10	Oct 29	Factoring	6.4
Week 11	Nov 5	Discrete Logarithms	7.1, 7.2
Week 12	Nov 12	Hash Functions	8.1, 8.2
Week 13	Nov 19	Elliptic Curves	16.1, 16.2
Week 14	Nov 26	Elliptic Curve Factoring	16.3
Week 15	Dec 3	Elliptic Curve Cryptosystems	16.5